REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

The provisional allowance of claims 7, 10, 20, 28 and 29 is appreciatively noted. These claims have been amended to self-standing format above and are thus assumed to be in fully allowed status.

It is also noted that there is no outstanding ground of rejection stated for claim 6. Accordingly, claim 6 has also been amended above to self-standing format and is presumed to be in allowable condition.

All other original claims have been cancelled without prejudice or disclaimer in favor of new claims 33-83.

New independent claim 33 is based upon a combination of original claims 3 and 5; new independent claim 49 is based upon a combination of original claims 3 and 6; and new independent claim 65 is based upon a combination of original claims 11, 12, 14, 17 and 18.

All of the outstanding grounds of rejection are respectfully traversed. However, except as noted below, all of such rejections are now believed to have been mooted and it is thus not believed necessary at this time to further explain reasons for such traversal.

Because of the relationship between the new claims and original claims noted above, it is presumed that the only outstanding grounds of rejection still pertinent to the new claims are allegations of obviousness under 35 U.S.C. §103 based on the combination of Allison '078 in view of Arnold '628 and/or the combination of Byers '290 in view of Arnold '628. Accordingly, those outstanding allegations are now discussed with respect to new independent claims 33, 49 and 65.

New claim 33 requires the provision of a public/private key pair valid only for a single communication between the authentication system and the receiving user. The required communication comprises: a message and/or response to the message; encryption of at lest part of the message using said public/private key pair; the sending of the public key to the receiving user as part of the message.

There is no suggestion in Arnold that the public/private key pairs generated for each user are single use only. Indeed, column 5, lines 53-62 and column 7, lines 50-53 suggest that key generation takes place only at registration. Additionally, there is no suggestion in Arnold that the public key is transmitted to the receiving user as part of the message. As is explained at column 6, lines 42-52, only the signature of the message, being the message digest encrypted with the private key is sent to the service provider and as is disclosed at column 8, lines 18 to 24 the message and the signature are encrypted by the service provider. In

neither case is it disclosed or suggested that the public key be incorporated into the message. As this is the case, new claim 33 is patentability distinguished over Allison in view of Arnold.

New claim 49 requires the provision of a public/private key pair valid only for a single communication between the authentication system and the receiving user. The required communication comprises: a message and/or a response to said message, the sending of said public key to said receiving user terminal prior to the communication and the store of the public key in the mobile terminal; and the encryption of at least part of the message using the public/private key pair. As discussed above, Arnold does not disclose or suggest the provision of a single use public/private key pair. New claim 49 is also patentably distinguished over Allison in view of Arnold.

New claim 65 requires that the message comprises: a first portion including the body of the message and a second portion containing encryption data used for encryption of the body and required for description of data included in the body. Arnold discloses at lines 38-52 at column 6 the transmission of a message comprising a body 202 and a signature 203, the body 202 being encrypted. The signature 203 comprises an encrypted message digest. The message disclosed in Arnold therefore does not contain encryption data nor an encrypted body.

At column 8, lines 18-24 Arnold discloses sending a message to recipients on the list of recipients. In this case, it appears that the whole message is encrypted. The message contents are listed as message ID, message text and message signature. There is no disclosure of the inclusion of encryption data used for encrypting the body and required for decrypting the body.

Therefore, Arnold does not disclose or suggest at least the feature of including in the message encryption data used for encrypting the body and required for decrypting the body. Accordingly, claim 65 is patentably distinguished over Byers in view of Arnold.

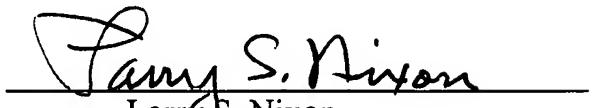
Dependent claims 34-48, 50-64 and 66-83 add yet further patentable distinction over the cited art.

The Examiner's attention is drawn to the attached Form PTO-1449 identifying documents that have been cited in recent search reports and official letters issued in corresponding UK and/or EPO proceedings and/or by the applicants own search effort. The IDS fee for this stage of prosecution is also attached. The undersigned is in the process of obtaining a copy of all non-US patent documents here identified and such copies will be supplied to the Examiner as soon as possible to complete this further disclosure. Applicant believes that the

now pending claims patentably distinguish over all prior art now of record and that, accordingly, an official Notice of Allowance is now in order.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Larry S. Nixon
Reg. No. 25,640

LSN:vc
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100